

Vanessa das Neves Pimentel

<Métodos de criptografia para sinais de voz>

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e de Telecomunicações da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Engenharia Elétrica e de Telecomunicações. Área de concentração: Sistemas de Telecomunicações.

Aprovada em maio de 2016.

BANCA EXAMINADORA

Prof. Edson Cataldo - Orientador, UFF

Prof. Wanderley Rezende, UFF

Prof. Leonardo Forero Mendoza, UERJ

Prof. Natalia Castro Fernandes, UFF

Niterói

2016

Dedicatória: Para Cacilda (In memoriam) e Leandro.

Agradecimentos

Primeiramente agradeço a Deus por mais uma etapa concluída em minha vida.

À minha mãe Cacilda (*in Memoriam*), agradeço pelo amor incondicional, os ensinamentos, a ajuda nas escolhas mais importantes da minha vida e o incentivo a crescer e me tornar o que sou hoje.

Ao meu marido Leandro, por todo amor e carinho, apoio, ajuda nos momentos mais difíceis, pelas palavras sábias e calmas, e principalmente o incentivo durante esta caminhada.

Aos meus amigos Nathália, Renata, Paola, Marly, Rodrigo e Thiago e a minha irmã Bianca, por serem tão especiais na minha vida, me entenderem nos momentos mais difíceis e me perdoarem pelas ausências.

Aos meus familiares, especialmente minha avó Maria, Cirleia (*in Memoriam*), Bárbara, Erika, Jorge, Renan, Kainan e meus afilhados Júlia e Arthur, por me apoiarem e entenderem que nem sempre estamos perto de quem amamos.

Ao meu orientador Edson Cataldo, pela oportunidade, ajuda, contribuição, orientação, confiança e disponibilidade ao longo desta etapa.

À CAPES pelo suporte financeiro.

Ao Curso de Pós-Graduação em Engenharia Elétrica e de Telecomunicações da Universidade Federal Fluminense pela oportunidade de aumentar meus conhecimentos.

Aos professores que fizeram e fazem parte da minha vida e que de alguma forma contribuíram para o meu conhecimento. Em especial, o professor Wanderley Rezende, pelo incentivo desde a época da graduação e pela confiança demonstrada, a professora Natalia Castro, pela disponibilidade e o apoio durante o mestrado, e aos professores Marcia Cerioli e Petrucio Viana, por me entenderem e me ajudarem nesta etapa.

Aos amigos de mestrado, especialmente ao Micahel e Fernando Otávio, agradeço pelos estudos e ajuda nos momentos mais desesperadores.

Resumo

A criptografia assegura a confidencialidade na troca de arquivos entre as partes envolvidas, sejam elas simples mensagens, áudios, vídeos ou mesmo arquivos mais complexos, mantendo a segurança e o sigilo das informações contidas nesses arquivos. Essa dissertação discute e implementa os métodos RSA e AES de criptografia para sinais de voz. A plataforma MATLAB foi usada para desenvolver os algoritmos e dois tipos de sinais de voz foram usados, a vogal /a/ e a palavra /aui/. Para cada método e para cada tipo de sinal de voz, as etapas de quantização, codificação, criptografia e decifragem foram implementadas. Para a quantização, foram considerados três métodos; quantização uniforme, quantização não-uniforme pela lei μ e quantização não-uniforme pela Lei A . Os resultados obtidos foram analisados e comparados. Um capítulo da dissertação é dedicado a discussão da criptografia quântica. Embora nenhuma implementação tenha sido realizada nesse caso, a sua discussão é importante devido a possibilidade de sua ampla aplicação no futuro.

Palavras-chave: Métodos de criptografia, Criptografia do sinal de voz, método RSA, método AES, criptografia quântica.

Abstract

Encryption ensures confidentiality in the exchange of files between the parties involved, whether simple messages, audio, video, or even more complex files, maintaining the security and confidentiality of the information contained in these files. This dissertation discusses and implements RSA and AES methods to voice files. The Matlab platform was used to develop the corresponding algorithms and two kinds of speech signals are used, the vowel / a / and the word / aui /. For each method and for each type of voice signal, the steps of quantization, encoding, encryption and decryption were implemented. For quantization, three methods were taken into account; uniform quantization, non-uniform quantization by law μ and non-uniform quantization by law A . The results were analyzed and compared. A chapter of the dissertation is devoted to discussion of quantum encryption. Although no implementation has been carried out in this case, its discussion is important because of the possibility of its wide application in the future.

Keywords: Encryption methods, voice signal encryption, RSA method, AES method, quantum encryption.

Lista de Figuras

3.1	Representação do processo de criptografia DES [40].	12
3.2	Tabela de permutação inicial inversa para DES [40].	13
3.3	Tabela de permutação inicial inversa para DES [40].	14
3.4	Processo de Cifragem e de Decifragem do algoritmo AES [40].	19
3.5	Processo de geração das oito primeiras posições da chave expandida AES [40].	23
3.6	Estrutura de uma rodada - AES [40].	26
3.7	Substituição entre a matriz de estado e a caixa-S - AES [40].	27
3.8	Substituição entre a matriz de estado e a caixa-S - AES [40].	29
3.9	Processo entre a matriz estado e a matriz da chave associada.- AES [40].	31
3.10	Algoritmo de decifragem equivalente- AES [40].	32
4.1	Algoritmo de gerações de chaves Diffie-Hellman [40].	38
6.1	Esquema do processo de criptografia e decifragem aplicado a um sinal da voz.	58
6.2	Parte do sinal original correspondente à emissão da vogal /a/.	62
6.3	Sinal quantizado obtido com a quantização uniforme correspondente à emissão da vogal /a/, para 8 bits.	63
6.4	Sinal codificado obtido com a quantização uniforme correspondente à emissão da vogal /a/, para 8 bits.	63
6.5	Sinal da vogal /a/ criptografado pelo método RSA, com quantização uniforme, 8 bits.	64
6.6	Sinal da vogal /a/ decifrado pelo método RSA, com quantização uniforme, 8 bits.	64

6.7	Sinal da vogal /a/ decodificado, com quantização uniforme, 8 bits.	64
6.8	Sinal da vogal /a/ original (linha cheia) e o sinal obtido ao fim do processo (linha tracejada), quantização uniforme, 8 bits.	65
6.9	Sinal da vogal /a/ original (linha cheia) e o sinal obtido ao fim do processo (linha tracejada), quantização uniforme, 16 bits.	66
6.10	Sinal da vogal /a/ original (linha cheia) e o sinal obtido ao fim do processo (linha tracejada), quantização uniforme, 30 bits.	67
6.11	Sinal da vogal /a/ original (linha cheia) e o sinal obtido ao fim do processo (linha tracejada), quantização uniforme, 60 bits.	67
6.12	Sinal quantizado obtido com a quantização não-uniforme lei μ correspondente à emissão da vogal /a/, para 8 bits.	68
6.13	Sinal codificado obtido com a quantização não-uniforme lei μ correspondente à emissão da vogal /a/, para 8 bits.	68
6.14	Sinal da vogal /a/ criptografado pelo método RSA, quantização não-uniforme lei μ , 8 bits.	68
6.15	Sinal da vogal /a/ decifrado pelo método RSA, quantização não uniforme lei μ , 8 bits.	69
6.16	Sinal da vogal /a/ decodificado, quantização não-uniforme lei μ , 8 bits.	69
6.17	Sinal da vogal /a/ original (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização não-uniforme, lei μ , 8 bits.	70
6.18	Sinal da vogal /a/ original (linha cheia) e o sinal obtido ao fim do processo (linha tracejada), quantização não-uniforme, lei μ , 16 bits.	70
6.19	Sinal quantizado obtido com a quantização não-uniforme lei A correspondente à emissão da vogal /a/, para 8 bits.	71
6.20	Sinal codificado obtido com a quantização não-uniforme lei A correspondente à emissão da vogal /a/, para 8 bits.	72
6.21	Sinal da vogal /a/ criptografado pelo método RSA, quantização não-uniforme lei A , 8 bits	72
6.22	Sinal da vogal /a/ decifrado pelo método RSA, quantização não-uniforme lei A , 8 bits	72

6.23	Sinal da vogal /a/ decodificado, quantização não-uniforme lei A , 8 bits. . .	73
6.24	Sinal da vogal /a/ original (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização não-uniforme, lei A , 8 bits.	73
6.25	Sinal da vogal /a/ original (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização não-uniforme, lei A , 16 bits.	74
6.26	Parte do sinal correspondente à emissão da palavra /aui/.	75
6.27	Sinal quantizado obtido com a quantização uniforme correspondente à emissão da palavra /aui/, para 8 bits.	75
6.28	Sinal codificado obtido com a quantização uniforme correspondente à emissão da palavra /aui/, para 8 bits.	76
6.29	Sinal da da palavra /aui/ criptografado pelo método RSA, quantização uniforme, 8 bits.	76
6.30	Sinal da da palavra /aui/ decifrado pelo método RSA, quantização uniforme, 8bits.	76
6.31	Sinal da da palavra /aui/ decodificado com quantização uniforme, 8bits. . .	77
6.32	Sinal original da palavra /aui/ (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização uniforme, 8 bits.	77
6.33	Sinal original da palavra /aui/ (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização uniforme, 16 bits.	78
6.34	Sinal quantizado obtido com a quantização não-uniforme lei μ correspondente à emissão da palavra /aui/, para 8 bits.	79
6.35	Sinal codificado obtido com a quantização não-uniforme lei μ correspondente à emissão da palavra /aui/, para 8 bits.	79
6.36	Sinal da palavra /aui/ criptografado pelo método RSA, quantização não-uniforme lei μ , para 8 bits.	80
6.37	Sinal da palavra /aui/ decifrado pelo método RSA, quantização não-uniforme lei μ , para 8 bits.	80
6.38	Sinal da da palavra /aui/ decodificado, quantização não uniforme lei μ , para 8 bits.	80
6.39	Sinal original da palavra /aui/ (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização não uniforme lei μ , 8 bits.	81

6.40	Sinal original da palavra /aui/ (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização não uniforme lei μ , 16 bits.	81
6.41	Sinal quantizado obtido com a quantização não uniforme lei A correspondente à emissão da palavra /aui/, para 8 bits.	82
6.42	Sinal codificado obtido com a quantização não-uniforme lei A correspondente à emissão da palavra /aui/, para 8 bits.	82
6.43	Sinal da palavra /aui/ criptografado pelo método RSA, quantização não-uniforme lei A , para 8 bits.	83
6.44	Sinal da palavra /aui/ decifrado pelo método RSA, quantização não uniforme lei A , para 8 bits.	83
6.45	Sinal da palavra /aui/ decodificado, quantização não uniforme lei A , para 8 bits.	83
6.46	Sinal original da palavra /aui/ (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização não uniforme lei A , para 8 bits.	84
6.47	Sinal original da palavra /aui/ (linha tracejada) e o sinal obtido ao fim do processo (linha cheia), quantização não uniforme lei A , para 16 bits.	85
6.48	Sinal da vogal /a/ criptografada pelo algoritmo AES, quantização uniforme.	87
6.49	Sinal da vogal /a/ decifrada pelo algoritmo AES pela quantização uniforme.	87
6.50	Sinal da vogal /a/ decodificado, quantização uniforme.	88
6.51	Sinal da vogal /a/ criptografada pelo algoritmo AES, quantização não-uniforme lei μ , para 8 bits.	88
6.52	Sinal da vogal /a/ decifrada pelo algoritmo AES, quantização não-uniforme lei μ , para 8 bits.	89
6.53	Sinal da vogal/a/ decodificado, quantização não-uniforme lei μ , para 8 bits.	89
6.54	sinal da vogal /a/ criptografada pelo algoritmo AES, quantização não-uniforme lei A , para 8 bits.	90
6.55	Sinal da vogal /a/ decifrada pelo algoritmo, AES quantização não-uniforme lei A , para 8 bits.	90
6.56	Sinal da vogal /a/ deccodificado, quantização não uniforme lei A , para 8 bits.	90

6.57 Sinal da palavra /aui/ criptografada pelo algoritmo AES, quantização uniforme, 16 bits	92
6.58 Sinal da palavra /aui/ decifrada pelo algoritmo AES, quantização uniforme, 16 bits.	92
6.59 Sinal da palavra /aui/ decodificado, quantização uniforme, 16 bits.	92
6.60 Sinal da palavra /aui/ criptografada pelo algoritmo AES, quantização não uniforme lei μ , 16 bits.	93
6.61 Sinal da palavra /aui/ decifrada pelo algoritmo AES, quantização não-uniforme lei μ , 16 bits.	93
6.62 Sinal da palavra /aui/ decodificada, quantização não-uniforme lei μ , 16 bits.	94
6.63 Sinal da palavra /aui/ criptografada pelo algoritmo AES, quantização não-uniforme lei A , 16 bits.	94
6.64 Sinal da palavra /aui/ decifrada pelo algoritmo AES, quantização não-uniforme lei A , 16 bits.	94
6.65 Sinal da palavra /aui/ decodificada, quantização não-uniforme lei A , 16 bits.	95

Lista de Tabelas

3.1	Tabela lógica da operação XOR	16
3.2	Valores possíveis da constante de rodada	24
3.3	Cálculo de uma chave de rodada	24
6.1	Valores dos números primos escolhidos no processo de criptografia pelo método RSA.	61
6.2	Valores dos números primos escolhidos no processo de criptografia pelo método RSA.	66

Sumário

1	Introdução	2
2	A criptografia: história, conceitos e desenvolvimento	5
2.1	Um pouco da história	5
2.1.1	Métodos criptográficos	8
3	Criptografia simétrica	10
3.1	Algoritmo DES	11
3.2	Algoritmo AES - Rijndael	14
3.2.1	A matemática do algoritmo AES	15
3.2.1.1	Adição e Multiplicação	15
3.2.2	Descrição do Algoritmo	17
3.2.2.1	Primeira Etapa	19
3.2.2.2	Segunda Etapa	25
3.2.2.3	Terceira Etapa	32
4	Criptografia assimétrica	37
4.1	Algoritmo RSA	39
4.1.1	A matemática do algoritmo RSA	40
4.1.1.1	Congruência Modular	40
4.1.1.2	Algoritmo de Euclides e o Algoritmo de Euclides Estendido	41
4.1.1.3	Teorema de Fermat	41
4.1.1.4	Teorema de Euler	41

4.1.1.5	Teorema Chinês do Resto	42
4.1.2	Geração de chaves	42
4.1.3	Criptografia de uma mensagem	43
4.1.4	Decifrando	44
5	Um pouco sobre a criptografia quântica	46
5.1	BB84	48
5.1.1	Descrição do protocolo BB84	49
5.1.2	Tentativa de Espionagem	52
5.1.3	Reconciliação de informação e amplificação de privacidade	53
5.1.4	Problemas de Implementação	54
6	Aplicação da criptografia a sinais de voz	57
6.1	Introdução	57
6.1.1	Quantização	58
6.2	Criptografia dos sinais de voz	60
6.2.1	Criptografia dos sinais de voz usando o método RSA	61
6.2.2	Criptografia de um sinal de voz correspondente à vogal /a/	62
6.2.2.1	Primeiro caso: vogal /a/ com quantização uniforme	62
6.2.2.2	Segundo caso: vogal /a/ quantização não-uniforme, Lei μ	67
6.2.2.3	Terceiro caso: vogal /a/ quantização não-uniforme, Lei A	71
6.2.3	Criptografia de um sinal de voz correspondente à palavra /aui/	75
6.2.3.1	Quarto caso: palavra /aui/ quantização uniforme	75
6.2.3.2	Quinto caso: palavra /aui/ quantização não uniforme, Lei μ	78
6.2.3.3	Sexto caso: palavra /aui/ quantização não-uniforme, Lei A	82
6.2.4	Criptografia dos sinais de voz usando o algoritmo AES	86

6.2.5	Criptografia de um sinal de voz correspondente à vogal /a/ pelo algoritmo AES	87
6.2.5.1	Primeiro Caso: quantização uniforme	87
6.2.5.2	Segundo Caso: quantização não uniforme pela Lei μ	88
6.2.5.3	Terceiro Caso: quantização não uniforme pela Lei A	89
6.2.6	Criptografia de um sinal de voz correspondente à palavra /aui/ pelo algoritmo AES	91
6.2.6.1	Quarto Caso: quantização uniforme	91
6.2.6.2	Quinto Caso: quantização não-uniforme pela Lei μ	93
6.2.6.3	Sexto Caso: quantização não uniforme pela Lei A	94
6.3	Comparação entre os resultados obtidos com os dois algoritmos	96
7	Conclusão e trabalhos futuros	99
	Referências Bibliográficas	101
	Referencias	102
	Apêndice A – Tabelas de permutações utilizadas pelo algoritmo DES	106
A.1	Permutação Inicial - IP	106
A.2	Permutação inicial inversa - IP^{-1}	107
A.3	Permutação da chave da rodada	107
A.4	Rotação - escalonamento de deslocamento à esquerda	107
A.5	Permutação de expansão	108
	Apêndice B – Caixa-S	109
	Apêndice C – Caixa-S Inversa	110
	Apêndice D – Rotina de Quantização Uniforme	111

Apêndice E - Rotina de Quantização Não Uniforme -Lei μ	114
Apêndice F - Rotina de Quantização Não Uniforme - Lei A	117
Apêndice G - Rotina do Algoritmo RSA	120
Apêndice H - Rotina do Algoritmo RSA para Lei μ	124
Apêndice I - Rotina do Algoritmo RSA para Lei A	128
Apêndice J - Rotina do Algoritmo AES	132